FOR IMMEDIATE RELEASE
July 10, 2025
Contact: Kaitlyn Palatucci, kpalatucci@it-isac.org

Food and Ag-ISAC and IT-ISAC Cyber Threat Bulletin: Iran-Israel Conflict

The Food and Ag-ISAC and IT-ISAC continue to monitor the potential cyber impacts from the ongoing Iran-Israel conflict. As of the distribution of this report, we have observed limited related attacks against U.S. companies, but are currently unaware of any attacks impacting our members. The information provided within this update is for situational awareness based on external reporting and open-source intelligence. While the ISAC strives to ensure accuracy and relevance, the details provided are subject to change as new information becomes available. Recipients should evaluate this intelligence in the context of their own risk assessments and operational environments.

In recent weeks, the ISACs have seen an uptick in reporting surrounding the following:

- Distributed denial-of-service (DDoS) attacks targeting Israeli banking, media, and transportation websites, likely driven by Iranian-aligned hacktivist collectives in retaliation for ongoing hostilities.
- Intrusions and disruptive operations against satellite and television broadcast infrastructure, intended to degrade communications and amplify psychological operations.
- Credential phishing campaigns targeting academic institutions, defense contractors, and technology providers, utilizing spoofed email invitations and malicious login portals.
- An Iranian ransomware group Pay2Key.I2P, which is a successor to Pay2Key has significantly ramped up its ransomware attacks, primarily targeting U.S. and Israeli entities.

Both ISACs caution that the cyber threat environment may remain highly volatile, with a risk of spillover to the private sector of countries allied with Israel and multinational organizations operating in or supporting Israel. The IT-ISAC and Food and Ag-ISAC have previously released two joint statements, highlighting the potential for cybersecurity impacts in response to the Middle Eastern conflict; these statements can be found on the website here.

IRANIAN THREAT ACTOR ACTIVITY

Based on current intelligence and historical activity, the following Iranian-aligned advanced persistent threats (APTs) and hacktivist collectives are most active or likely to escalate operations.

APT35 (Charming Kitten)
APT35 is believed to be connected to the Iranian Revolutionary Guard Corps (IRGC). The group is known for extensive cyber espionage and intelligence gathering activities, which support Iran's strategic priorities. APT35 often uses social engineering tactics to target government, diplomatic, and military personnel, academia and researchers, journalists and media organizations, political dissidents, and critical infrastructure, including the defense, energy, and telecommunications sectors.

- **Focus:** Credential harvesting and espionage against academia, defense, and NGOs.
- **Methods**: Spearphishing with fake conference invitations and credential phishing portals.

APT34 (OilRig)
APT34 is known for its development of custom malware, targeted spearphishing campaigns, and for social engineering supply chain entities to pivot to higher-value targets. Aside from impersonating various entities for social engineering attacks, the group is also known to leverage known vulnerabilities for initial access. APT34 historically has targeted organizations in the financial sector, oil and gas, chemical, telecommunications, and various other critical industries.

- **Focus:** Financial, energy, and telecom sectors.
- **Methods:** Malware implants, supply chain compromise, and credential theft.

APT39 (Chafer)
Strongly linked to the Iranian Ministry of Intelligence and Security (MOIS), the group is known for its cyber espionage capabilities. While other Iranian nation-state groups focus on cyber espionage and intelligence gathering, APT39 has displayed more specific skills towards monitoring, tracking, and surveillance operations against specific targets. They have impacted telecommunications companies to collect customer data and potentially facilitate surveillance; infiltrated travel and hospitality organizations to track individuals, including obtaining travel itineraries and personal information; and targeted high-tech companies and IT firms that support these sectors.

- **Focus:** Personal data collection, telecom targeting, and surveillance.
- **Methods:** Credential collection and long-term access operations.

Imperial Kitten (Tortoiseshell)
Also linked to the Islamic Revolutionary Guard Corps (IRGC), Imperial Kitten typically targets IT service providers (ITSPs) and managed service providers (MSPs) to gain access to downstream customers. The group is known for its extensive use of social engineering, often in the form of job recruitment themes to deliver malware to victims. They also develop a set of custom malware and commodity tools for later stages of their attacks.

- **Focus:** IT providers and defense contractors.
- **Methods:** Custom remote access tools and strategic web compromises.

Moses Staff
The line between Iranian hacktivist groups and nation-state groups can be blurry, as groups like Moses Staff have shown strong links to the Iranian government. Many of the group's activities show an intention to advance Iran's strategic goals. Moses Staff is known for destructive attacks against Israeli organizations, using data encryption and shaming through public data leaks to impart psychological impacts to adversarial nations.

- **Focus:** Data leaks and destructive attacks targeting Israeli organizations.
- **Methods:** Data encryption and public leaks for psychological impact.

CyberAv3ngers (Black Shadow)
Another prominent hacktivist group coming from Iran is CyberAv3ngers. The group is known for disruptive and destructive attacks against Iranian adversaries. Notably, during the Israel/Gaza conflict, the CyberAv3ngers leveraged a vulnerability in an Israeli-made programmable logic controller (PLC) to impact critical infrastructure in the U.S.

- **Focus:** DDoS and data leaks against critical infrastructure and public services.
- **Methods:** Website defacement, disruptive operations, and Telegram-based leaks.

Iranian Hacktivist Collectives
These collectives include various loosely affiliated groups mobilizing around geopolitical flashpoints.

- **Methods:** DDoS attacks, defacements, and hack-and-leak campaigns.

RECENT CYBER INCIDENTS IN THE CURRENT IRAN-ISRAEL CONFLICT

Iranian APTs Increased Activity Against US Industries in Late Spring

- **Event:** Nozomi Networks found attacks from Iranian adversaries increased to 28 between May and June, up from 12 attacks in the previous two months. The researchers did not share who the victims of the attacks were, but identified the attacks as coming from several well-known Iranian advanced persistent threat (APT) groups. Specifically, MuddyWater, APT33, OilRig, CyberAv3ngers, FoxKitten and Homeland Justice. The attacks impacted primarily the transportation and manufacturing sectors.
- **Significance:** Nozomi Networks noted that the most active group was MuddyWater, which targeted at least five US companies. Following MuddyWater was APT33, which was responsible for attacks against three firms. The takeaway from this report is that not just hacktivist collectives have turned their sights on Western entities, but also advanced persistent actors from Iran.
- **Sources:**
  - https://www.nozominetworks.com/blog/threat-actor-activity-related-to-the-iran-conflict
  - https://therecord.media/iran-state-backed-hackers-industrial-attacks-spring-2025

Pay2Key.I2P Ransomware (Israel and US)

- **Event:** Morphisec reports that Pay2Key.I2P, a group linked to the Fox Kitten APT group, has significantly ramped up its ransomware attacks, primarily targeting U.S. and Israeli entities. Pay2Key.I2P emerged in February 2025, likely serving as a successor to Pay2Key. Since its entrance to the ransomware scene, the ransomware-as-a-service (RaaS) operation has targeted over 50 organizations and secured roughly $4 million dollars in ransom payments.
- **Significance:** Morphisec notes that the ransomware strain shares some similarities with Mimic ransomware. It is known to use a complex loader script to evade detection and will disable Microsoft Defender to drop payloads. With escalating cyber threats coming from Iranian-based actors, there are concerns that the ransomware group will set its sights on US critical infrastructure.
- **Source:**
  https://engage.morphisec.com/hubfs/Pay2Key_Iranian_Cyber_Warfare_Targets_the_West_Whitepaper.pdf

State TV Broadcast Hijacking (Iran)

- **Event:** On June 18, 2025, Iranian state television was briefly hijacked. Attackers aired footage of women's protests and messages urging public uprising. Iranian officials blamed Israeli-linked actors known as "Lion's Awakening," who likely used satellite signal interference.
- **Significance:** Demonstrates the use of media manipulation as a psychological operation to undermine regime credibility.
- **Sources:**
  - https://www.i24news.tv/en/news/israel/defense/artc-iranian-tv-hacked-protest-footage-aired-israel-blamed-for-cyber-offensive
  - https://zendata.security/2025/06/24/zendatas-cyber-analysis-of-the-iran-israel-conflict

Hijacking of Home and CCTV Cameras (Israel)

- **Event:** Iranian-linked actors attempted to connect to Israeli home security and CCTV camera systems. This appeared aimed at monitoring missile strike impacts in real time.
- **Significance:** Illustrates how attackers exploit the internet of things (IoT) vulnerabilities for situational awareness in conflict zones.
- **Source:**
  https://industrialcyber.co/industrial-cyber-attacks/researchers-warn-of-escalating-cyber-threats-as-iranian-hackers-hijack-cameras-target-israeli-infrastructure

DDoS Attacks on Israel and the U.S.

- **Israel:** From June 4 - 12, 2025, researchers observed 3 to 4 DDoS attacks daily, peaking at 34 incidents per day after June 13. These accounted for about 40% of all known hacktivist-driven DDoS attacks globally during that period.
- **United States:** Between June 21 - 22, 2025, Iranian-aligned and sympathetic hacktivists, including Mr. Hamza, Mysterious Team Bangladesh, and Keynous, launched significant attacks on U.S. organizations. The attacks caused an estimated 800% surge in observed DDoS traffic.
- **Significance:** Highlights a spillover of disruption targeting allies and Western infrastructure.
- **Sources:**
  - https://www.darkreading.com/threat-intelligence/iran-israel-war-maelstrom-cyberspace
  - https://www.techradar.com/pro/security/mr-hamza-mysterious-team-bangladesh-and-keynous-led-a-massive-surge-in-ddos-on-us-businesses-following-an-attack-on-iran

Cryptocurrency Platform and Bank Disruption (Iran)

- **Event:** The group “Predatory Sparrow” is suspected of destroying around $90 million in cryptocurrency on Nobitex and wiping data at Iran’s Bank Sepah.
  Significance: Represents one of the most impactful financial sabotage operations in recent regional cyber conflicts.
- **Source:**
  - https://www.wsj.com/world/middle-east/how-israel-aligned-hackers-hobbled-irans-financial-system-fb1b0376

RECOMMENDED MITIGATION MEASURES

- Increase monitoring for spearphishing and credential theft.
- Review DDoS mitigation playbooks, and ensure response partners are on standby.
- Validate backup and recovery processes for critical systems, especially in your communications infrastructure.
- Remain vigilant for signs of supply chain compromise or attempts to leverage trusted relationships for lateral movement.
- Enable multi-factor authentication (MFA) wherever possible.

###

About the Food and Ag-ISAC
Founded in 2023, the Food and Agriculture-Information Sharing and Analysis Center (Food and Ag-ISAC) provides threat intelligence, analysis, and effective security practices that help food and agriculture companies detect attacks, respond to incidents, and share indicators so they can better protect themselves and manage risks to their companies and the sector.

For more information about the Food and Ag-ISAC, please visit www.foodandag-isac.org.
- X: x.com/foodandagisac
- LinkedIn: www.linkedin.com/company/food-agriculture-isac

About the IT-ISAC
Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies. We serve as a force multiplier that enables collaboration and sharing of relevant, actionable cyber threat intelligence, effective security policies, and practices for the benefit of all.

For more information about the IT-ISAC, please visit www.it-isac.org.
- X: x.com/itisac
- LinkedIn: www.linkedin.com/company/it-isac